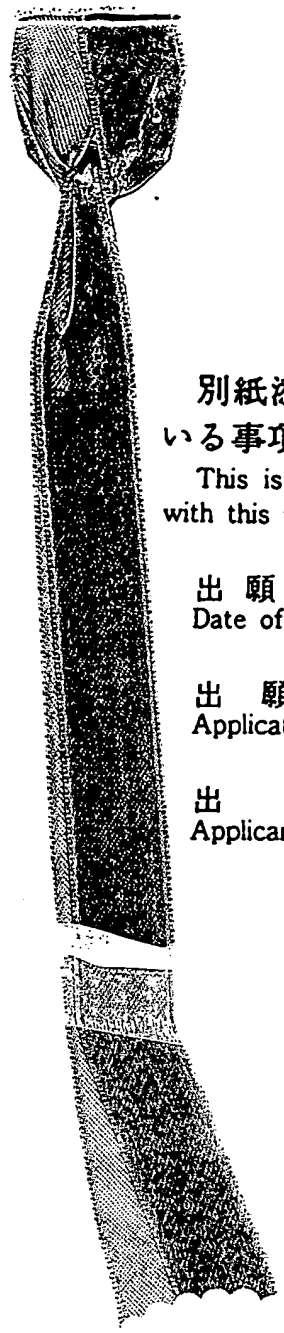


04-0024-TH(2)

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２６日

出願番号
Application Number: 特願２０００－０１６９３７

出願人
Applicant (s): 日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　412000058

【提出日】　平成12年 1月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/08

G09C 1/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　猪羽　渉

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　日暮　誠司

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　黒岩　俊夫

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　上田　健二朗

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【電話番号】　045-450-2423

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法

【特許請求の範囲】

【請求項１】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、

前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報又は前記鍵情報の一部として出力する第２ステップとからなることを特徴とする鍵情報生成方法。

【請求項２】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、

前記鍵情報を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、

前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報又は前記鍵情報の一部として出力する論理演算部とを備えたことを特徴とする鍵情報生成装置。

【請求項３】

第１鍵のもとになる情報を第２鍵で暗号化すると共に、前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則

に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、

前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する第２ステップとからなることを特徴とするコンテンツ情報暗号化方法。

【請求項４】

第１鍵のもとになる情報を第２鍵で暗号化すると共に、前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、

前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数よ

り少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報暗号化装置。

【請求項５】

暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、

前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する第２ステップとからなることを特徴とするコンテンツ情報復号化方法。

【請求項６】

暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、

前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報復号化装置。

【請求項７】

請求項３記載のコンテンツ情報暗号化方法、もしくは、請求項４記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを記録媒体に記録したことを特徴とするコンテンツ情報記録媒体。

【請求項８】

請求項３記載のコンテンツ情報暗号化方法、もしくは、請求項４記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第

１鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツ情報を暗号化したり、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する、鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法に関するものである。

【０００２】

【従来の技術】

近年、ディジタル化が進み、ディジタル化された映像信号や音声情報などのコンテンツ情報を記録媒体に記録して再生したり、あるいは、ソフトウェアやデータなどのコンテンツ情報をネットワークにより伝送することが盛んに行われている。

【０００３】

そして、著作権を有し且つディジタル化されたコンテンツ情報（以下、ディジタル情報と記す）の不正使用を防止する場合、ディジタル情報に対して所定の暗号化鍵を用いて暗号化し、この暗号化したディジタル情報を磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体に記録したり、あるいは、暗号化したディジタル情報をネットワークを介して伝送したりしている。この後、記録媒体やネットワークを介して提供された暗号化済みのディジタル情報は、暗号化鍵と等価の復号化鍵を用いて復号化されて暗号化前のディジタル情報に戻している。

【０００４】

一方、ＤＥＳ（Data Encryption Standard）暗号化方法は、アメリカ商務省標準局（現在、ＮＩＳＴ：National Institute of Standard Technology ）が決めた暗号標準であり、現在もつとも多く用いられている暗号化方法の一つである。このＤＥＳ暗号化方法では、６４ビット平文入力が６４ビット暗号文出力に変換

される。この際、暗号化鍵も平文入力と同じように６４ビット構成であるが、そのうちの８ビットをパリティに使っているので、実質的な暗号化鍵は５６ビット構成となっている。

【０００５】

図４は一般的なＤＥＳ（Data Encryption Standard）暗号化方法に用いられているＳ－Ｂｏｘを示したブロック図である。

【０００６】

図４に示した如く、ＤＥＳ（NIST.FIPS Publication 46-1:Data Encryption Standard.January 22,1988）暗号化方法に用いられているＳ－Ｂｏｘ（Selection －Box ）は、６ビットの入力に対して４ビットを出力する、一方向性関数の一種である。この種の一方向性関数Ｆは、一方向性ハッシュ関数（One-Way Hash Function)、又は単に、ハッシュ関数と呼ばれる、ｘからＦ（ｘ）を計算するのは容易であるが、Ｆ（ｘ）からｘを求めるのは極めて困難な関数Ｆ（ｘ）を用いている。

【０００７】

また、上記したＳ－Ｂｏｘは二次元のテーブルＴを持っていて、４行×１６列のテーブルＴ内に行と列とに対応させて各要素値Ｈが０から１５までの１６進の整数で予め設定されている。そして、入力の６ビットを例えば“$b_5b_4b_3b_2b_1b_0$”とすると、“b_5”と“b_0”の２ビットでテーブルＴの行を指定し、また“b_5”と“b_0”の２ビットを除いた“$b_4b_3b_2b_1$”の４ビットでテーブルＴの列を指定し、ここで指定した行列の部位と対応して４ビットからなる一つの要素値Ｈを出力している。

【０００８】

上記した具体例を図４に示すと、Ｓ－Ｂｏｘへの入力６ビットを例えば“１００１００”とした時、“１０”行“００１０”列、すなわち、２行２列の要素値９（＝１００１）を出力している。

【０００９】

【発明が解決しようとする課題】

ところで、公知のＳ－Ｂｏｘを用いて鍵のもとになる情報から、暗号化及び復

号化に必要な暗号化鍵及び復号化鍵を生成するために必要な一方向性関数を求めようとする場合、上記したＳ－Ｂｏｘでは入力ビットの“０”と“１”との割合を直接反映しないでテーブルＴから出力を得ることができるので、これを用いて暗号化鍵及び復号化鍵の生成に好適なシステムを実現することが可能である。

【００１０】

しかしながら、暗号化及び復号化に必要な暗号化鍵及び復号化鍵を生成する際に、上記したＳ－Ｂｏｘにより例えば６ビットの入力に対して４ビットを出力するのでは、一定のビット数を減らす一方向性関数しか構成できず、しかも、少ないステップ数で大きなビット数の入力に対して小さなビット数に減らし、かつ任意にその圧縮率を変えられるような一方向性関数を構成することはできないなど問題点が生じている。

【００１１】

【課題を解決するための手段】

本発明は上記課題に鑑みてなされたものであり、第１の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より

少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報又は前記鍵情報の一部として出力する第２ステップとからなることを特徴とする鍵情報生成方法である。

【００１２】

また、第２の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、

前記鍵情報を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、

前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報又は前記鍵情報の一部として出力する論理演算部とを備えたことを特徴とする鍵情報生成装置である。

【００１３】

また、第３の発明は、第１鍵のもとになる情報を第２鍵で暗号化すると共に、前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第

１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する第２ステップとからなることを特徴とするコンテンツ情報暗号化方法である。

【００１４】

また、第４の発明は、第１鍵のもとになる情報を第２鍵で暗号化すると共に、前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビッ

ト列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報暗号化装置である。

【００１５】

また、第５の発明は、暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果

のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する第２ステップとからなることを特徴とするコンテンツ情報復号化方法である。

【００１６】

また、第６の発明は、暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第１鍵を生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、

前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記第１鍵又は前記第１鍵の一部として出力する論理演算部とを備えたことを特徴とするコンテンツ情報復号化装置である。

【００１７】

また、第７の発明は、上記した第３の発明のコンテンツ情報暗号化方法、もしくは、第４の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを記録媒体に記録したことを

特徴とするコンテンツ情報記録媒体である。

【００１８】

また、第８の発明は、上記した第３の発明のコンテンツ情報暗号化方法、もしくは、第４の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法である。

【００１９】

【発明の実施の形態】

以下に本発明に係る鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法の一実施例を図１乃至図３を参照して詳細に説明する。

【００２０】

図１は本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【００２１】

まず、図１を用いて本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法について説明する。

【００２２】

図１において、記録側または送信側とは、著作権を有するコンテンツ情報（以下、ディジタル情報と記す）を暗号して、暗号化したディジタル情報を磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体（コンテンツ情報記録媒体）に記録する側を示し、または、暗号化したディジタル情報をネットワーク（インターネット，電話回線），電波，光無線などの伝送路に送信する側を示しており、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置と対応する側である。

【００２３】

一方、再生側または受信側とは、記録側で暗号化したコンテンツ情報を記録した記録媒体を再生する側を示し、または、送信側で暗号化したコンテンツ情報を伝送路を介して受信する側を示しており、コンテンツ情報復号化方法、コンテンツ情報復号化装置と対応する側である。

【００２４】

まず、記録側または送信側において、ディジタル化された映像信号や音声情報など著作権を有するディジタル情報０４は、暗号化鍵である第１鍵Ｋ１を用いて第１暗号化装置０５によって暗号化される。この際、第１鍵Ｋ１は、第１鍵のもとになる情報０１から後述する一方向性関数０３を用いて生成される。

【００２５】

また、第１鍵のもとになる情報０１は、システム固有の第２鍵（以下、システム鍵と記す）Ｋ２を用いて暗号化される。このシステム鍵Ｋ２は、システム固有のＩＤなどを用いて生成した暗号化鍵である。

【００２６】

そして、第１鍵Ｋ１を用いて第１暗号化装置０５によって暗号化したディジタル情報０７と、システム鍵Ｋ２を用いて第２暗号化装置０２によって暗号化した第１鍵のもとになる情報０６とが、記録側で磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体に記録されて再生側に提供されるか、または、ネットワーク（インターネット，電話回線），電波，光無線などの伝送路を介して送信されて受信側で受信される。

【００２７】

次に、再生側または受信側において、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化された第１鍵のもとになる情報０６は、第２復号化装置０８でシステム固有の第２鍵（システム鍵）Ｋ２を用いて第１鍵のもとになる情報０９に復号化される。ここで用いられるシステム鍵Ｋ２も、システム固有のＩＤなどを用いて生成した復号化鍵であり、且つ、記録側または送信側で暗号化時に用いたシステム鍵Ｋ２と等価のものである。

【００２８】

また、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化さ

れたディジタル情報０７は、復号化鍵である第１鍵Ｋ１を用いて第１復号化装置１１で元のディジタル情報（コンテンツ情報）１２に復号化される。この際、第１鍵Ｋ１は、第２復号化装置０８から出力された復号化後の第１鍵のもとになる情報０９から後述する一方向性関数１０を用いて生成され、且つ、記録側または送信側で暗号化時に用いた第１鍵Ｋ１と等価のものである。

【００２９】

上記した暗号化及び復号化において、システム鍵Ｋ２は予め、記録側または送信側と、再生側または受信側で共通になるよう設定しておいても良く、更に、既知の公開鍵暗号方式や鍵配送方式を用いてもかまわない。

【００３０】

次に、本発明の要部をなす上記した第１鍵Ｋ１を生成する鍵情報生成方法及び鍵情報生成装置について、図２乃至図３を用いて説明する。

【００３１】

図２は図１に示した第１鍵を生成する鍵情報生成方法を説明するための具体例を示した図、

図３は第１鍵を生成する鍵情報生成装置の具体例を示したブロック図である。

【００３２】

上記したように、第１鍵Ｋ１は暗号化前のディジタル情報０４への暗号化及び暗号化したディジタル情報０７への復号化に用いられる鍵情報であり、この第１鍵Ｋ１は先に説明した一方向性関数０３，１０を適用しているものの、本発明に係る鍵情報生成方法及び鍵情報生成装置では、従来技術で説明したＤＥＳ暗号化方法におけるＳ－Ｂｏｘを適用した第１ステップと、本発明で新たに開発した第２ステップとを組み合わせて第１鍵Ｋ１を生成することを特徴とするものである。

【００３３】

まず、図２に示した本発明に係る鍵情報生成方法は、一方向性関数を用いて第１鍵Ｋ１を生成するにあたって、第１鍵のもとになる情報０１（又は０９）を入力して、ここで入力した多数のビットからなるビット列を基にして、第１，第２ステップを経て、第１ステップで入力したビット列のビット数より極めて少ない

ビット数のビット列を生成して、これを第１鍵Ｋ１にすることを示している。

【００３４】

即ち、図２及び図３に示した本発明に係る鍵情報生成方法及び鍵情報生成装置の具体例において、まず、第１ステップでは従来技術で説明したＤＥＳ暗号化方法におけるＳ－Ｂｏｘを適用している。

【００３５】

上記した第１ステップにおいて、多数のビットからなる第１ビット列を有する第１鍵のもとになる情報０１（又は０９）を、この第１ビット列よりビット数が少ない複数のビットを有する第２ビット列に順次分割して、分割した各第２ビット列を鍵情報生成装置３０に設けたＳ－Ｂｏｘ３１に分割した順に入力している。

【００３６】

また、上記したＳ－Ｂｏｘ３１は内部に二次元のテーブルＴを持ち、且つ、テーブルＴは、従来例で説明したと同様に、指定した行列の各部位に対応して第２ビット列より少ないビット数からなる一つの要素値Ｈが予め設定されている。

【００３７】

ここで、入力した各第２ビット列ごとに、第２ビット列の複数のビットを用いて所定の規則に従ってテーブルＴの行と列とを指定している。この際、第２ビット列の複数のビットを用いてテーブルＴの行と列とを指定するための所定の規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

【００３８】

そして、分割した一つの第２ビット列によって指定された行列に対応した部位から一つの要素値Ｈを後述する第２ステップ側の論理演算部３２側に出力し、これを分割した各第２ビット列ごとに繰り返して複数の要素値Ｈで合成した第３ビット列を論理演算部３２側への入力としている。

【００３９】

これにより、第１ステップでは、多数のビットを有する第１ビット列からこれよりビット数が少ない第２ビット列に順次分割した後に、分割した各第２ビット

列をＳ－Ｂｏｘ３１に順次入力して、Ｓ－Ｂｏｘ３１から出力する時には入力した第１ビット列よりビット数が少ないビット数の第３ビット列に変換されることになる。

【００４０】

即ち、具体例における第１ステップにおいて、第１鍵のもとになる情報０１（又は０９）は、各ビットが“０”又は“１”のバイナリーデータで例えば２００ビットからなる第１ビット列を形成しており、この第１ビット列を例えば８ビットを有する第２ビット列に順次分割して、２５個の第２ビット列をＳ－Ｂｏｘ３１に順次入力している。

【００４１】

ここで、Ｓ－Ｂｏｘ３１に入力した１番目の第２ビット列が例えば$a_1a_2a_3a_4a_5a_6a_7a_8$とすると、８ビットの$a_1a_2a_3a_4a_5a_6a_7a_8$のうちで$a_1a_2a_3a_4$の４ビットでテーブルＴの行を指定し、$a_5a_6a_7a_8$の４ビットでテーブルＴの列を指定している。

一方、テーブルＴ内では、第２ビット列により指定した行列に対応した部位の要素値Ｈを０から１５までの整数、すなわち１６進数で表せば、０からｆの４ビットの値として予め設定されている。

そして、１番目の第２ビット列で指定した行列に対応した部位（$a_1a_2a_3a_4$行$a_5a_6a_7a_8$列成分）の４ビットからなる１番目の要素値Ｈとして$b_{11}b_{12}b_{13}b_{14}$をＳ－Ｂｏｘ３１から出力し、この後、２番目の第２ビット列で２番目の要素値Ｈとして$b_{15}b_{21}b_{22}b_{23}$を出力し、更にこの後、上記した第１ステップを２３回繰り返して、ここで得られた全部で２５個の各要素値Ｈを合成することで、入力した第１ビット列よりビット数が少ない１００ビットからなる第３ビット列が得られ、これを後述する第２ステップの論理演算部３２側への入力ビット列としている。

【００４２】

尚、上記した第１ステップでは、２００ビットの第１ビット列を８ビットつづ分けて説明したが、入力した第１ビット列のビット数及び第１ビット列を分割した第２ビット列のビット数は適宜設定されるものである。また、第１ビット列を

分割した各第２ビット列を同一のテーブルＴで上記と同様に処理するか、または、異なるテーブルで処理しても良い。更に、テーブルＴ内の各要素値Ｈは、入力ビット数より少ないビット数で０から１５以外の数を出力値として設定しても良い。

【００４３】

次に、本発明で新たに開発した第２ステップでは、第１ステップで得られた複数のビットを有する第３ビット列を鍵情報生成装置３０に設けた論理演算部３２にそのまま入力するか、又は、第３ビット列より少ないビット数からなる第４ビット列に順次分割して、分割した複数の第４ビット列のうちで一部の第４ビット列を論理演算部３２に入力するか、もしくは、複数の第４ビット列を論理演算部３２に順次入力している。

【００４４】

上記した論理演算部３２では、入力した第３又は第４ビット列の各ビットを、行列を有する第１マトリックスＭ１内に所定の配列規則に従って配置している。この際、第１マトリックスＭ１内に第３又は第４ビット列の各ビットを配置するための所定の配列規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

この後、第１マトリックスＭ１内で入力した第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに順に論理演算する。そして、論理演算して得られた各結果のビットを、第１マトリックスＭ１より行列を小さくした第２マトリックスＭ２内にブロック順に配置して、第２マトリックスＭ２内の各ビットから第３又は第４ビット列のビット数より少ないビット数の第５ビット列を生成して第１鍵Ｋ１又は第１鍵Ｋ１の一部として出力している。

【００４５】

これにより、第２ステップでは、第１ステップで得られた第３ビット列又は第３ビット列よりビット数を少なくして分割した第４ビット列を論理演算部３２に入力して、論理演算部３２から出力する時には、第１，第２ステップの入力ビットよりビット数が少ない第５ビット列に変換されて、第１鍵Ｋ１又は第１鍵Ｋ１

の一部として出力されることになる。

【００４６】

即ち、具体例における第２ステップでは、第１ステップで得られた１００ビットを有する第３ビット列を例えば２５ビットごとに分割し、分割して得られた第３ビット列を論理演算部３２に入力している。

【００４７】

尚、具体例における第２ステップで第１ステップで得られた第３ビット列を論理演算部３２にそのまま入力する場合には、第３ビット列のビット数が第１ステップの入力ビット数よりも少なく、しかも、この第３ビット列をこれより少ないビット数に分割する必要がない場合であるが、この第３ビット列の複数のビットを第１マトリックスＭ１内に所定の配列規則に従って配置して以下の記載と同様に処理するものであるので、この場合の説明を省略する。

【００４８】

ここで、第１ステップで得られた１００ビットを有する第３ビット列から分割して１番目に入力した２５ビットの第４ビット列を、最上位から順に$b_{11}b_{12}b_{13}b_{14}b_{15}b_{21}b_{22}b_{23}b_{24}b_{25}\cdots\cdots b_{51}b_{52}b_{53}b_{54}b_{55}$とし、各ビットの値は“０”又は“１”のバイナリデータとする。

【００４９】

そして、入力した２５ビットからなる第４ビット列のうちで例えば$b_{11}b_{12}b_{13}b_{14}b_{15}$を第１マトリックスＭ１内の第１行目に列に沿って配置し、$b_{21}b_{22}b_{23}b_{24}b_{25}$を第２行目に列に沿って配置し、以下同様に順次繰り返して、$b_{51}b_{52}b_{53}b_{54}b_{55}$を第５行目に列に沿って配置することで、入力した各ビットを第１マトリックスＭ１内に５×５のビットマトリックスとして配置している。

【００５０】

この後、第１マトリックスＭ１内で入力した第４ビット列のビット数より少ないビット数で例えば$b_{11}b_{12}b_{21}b_{22}$を第１ブロックとして形成して、b_{11}とb_{12}とb_{21}とb_{22}とで排他的論理和を取り、この排他的論理和の結果のビットc_{11}を第２マトリックスＭ２内の第１行，第１列目に配置する。次に、第１ブロックに対して列を１列ずらした$b_{12}b_{13}b_{22}b_{23}$を第２ブロックとして形成して、上

記と同様に論理演算した結果のビットc_{12}を第２マトリックスＭ２内の第１行第２列目に配置する。上記のように、列方向に沿って４ブロックの論理演算処理が終わったら、１行ずらして再び上記処理を順次繰り返し、合計で１６ブロックの論理演算処理が全て終了すると、第２マトリックスＭ２内に４×４のビットマトリックスが形成される。この後、第２マトリックスＭ２内の４×４のビットマトリックスから第５ビット列として１６ビットからなる$c_{11}c_{12}c_{13}c_{14}c_{21}c_{22}c_{23}c_{24}c_{31}c_{32}c_{33}c_{34}c_{41}c_{42}c_{43}c_{44}$を生成して、この第５ビット列を論理演算部３２から第１鍵Ｋ１として出力するか、又は、第１鍵Ｋ１の一部として出力している。

【００５１】

この際、論理演算部３２から第１鍵Ｋ１の一部として出力する場合には、１番目の第４ビット列以外の残りのいくつかの第４ビット列を上記と同様に処理して、これらを合成して最終的に第１鍵Ｋ１として論理演算部３２から出力するものであり、例えば１番目～４番目の第４ビット列を用いた場合には第１鍵Ｋ１が６４ビットとなり、この場合でも第１鍵Ｋ１は第１，第２ステップで入力したビット数よりも少ないビット数に削減されている。

【００５２】

尚、具体例における第２ステップでは、論理演算部３２に入力した第４ビット列のビット数を２５ビットとしたがこれに限ることなく、第１ステップの入力ビット数より少ない適宜なビット数でも良い。また、第１マトリックスＭ１内で入力した２５ビットを第４ビット列の最上位から最下位に向かって順に配置して説明したが、これに限ることなく、所定の配列規則に従って配置しても良い。また、第１マトリックスＭ１内に形成した各ブロックごとの論理演算も排他的論理和（ＥＸ－ＯＲ）に代えて論理和（ＯＲ）又は論理積（ＡＮＤ）で行っても良い。

【００５３】

そして、論理演算部３２から出力され、一方向性関数により生成された第１鍵Ｋ１は、第１暗号化装置０５でディジタル情報０４の暗号化に用いられ、また、第１復号化装置１１で暗号化したディジタル情報０７の復号化に用いられている。　尚、実施例では暗号化を２段としたが、第ｎ－１鍵（但し、ｎは３以上の整

数）のもとになる情報を第ｎ暗号化装置で暗号化する場合、第ｎ鍵をのもとになる情報から第ｎ鍵を生成するのに、上記の一方向性関数を用いたシステムを構築することも可能である。

【００５４】

【発明の効果】

以上詳述した本発明に係る鍵情報生成方法、コンテンツ情報暗号化方法、コンテンツ情報復号化方法によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第１鍵）を、鍵（第１鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力する第１ステップと、前記第１ステップで出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報（第１鍵）又は前記鍵情報（第１鍵）の一部として出力する第２ステップとで行っているので、本発明により容易にシステムに応じた量のビット数を少ないステップ数でかつセキュリティを保持したまま減少させることが可能な一方向性関数を実現することができる。そしてこの一方向性関数は入力ビットの“０”と“１”の割合を出力に直接反映させないため、暗号化鍵及び復号化鍵に利用するのに好適で、かつ

鍵（第１鍵）のもとになる情報は必要な鍵のサイズに関係なく設定することが可能となる。また、一方向性関数内のビット演算の方法や置換によって、より鍵生成のメカニズムのセキュリティを高めることができる。

【００５５】

また、本発明に係る鍵情報生成装置、コンテンツ情報暗号化装置、コンテンツ情報復号化装置によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第１鍵）を、鍵（第１鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、多数のビットからなる第１ビット列を有する前記鍵のもとになる情報を、前記第１ビット列よりビット数の少ない複数のビットからなる第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数からなる各要素値を予め設定しておき、順次入力した各前記第２ビット列の複数のビットを用いて所定の規則に従って前記テーブルの行と列とを指定すると共に、順次入力した各前記第２ビット列で指定した行列の部位と対応して得た各前記要素値を合成して前記第１ビット列よりビット数が少ないビット数の第３ビット列を出力するＳ－Ｂｏｘと、前記Ｓ－Ｂｏｘから出力した前記第３ビット列を入力するか、又は前記第３ビット列をこれよりビット数が少ないビット列に分割した第４ビット列を入力し、前記第３又は第４ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第３又は第４ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第３又は第４ビット列のビット数より少ないビット数の第５ビット列を前記鍵情報（第１鍵）又は前記鍵情報（第１鍵）の一部として出力する論理演算部とを備えているので、上記した各方法で述べた効果と同様の効果を得ることができる。

【００５６】

また、本発明に係るコンテンツ情報記録媒体、コンテンツ情報伝送方法によれば、上記した第１鍵を用いて暗号化したコンテンツ情報と、暗号化した第１鍵のもとになる情報とを記録媒体に記録するか、または、伝送路を介して送信してい

るので、コンテンツ情報のセキュリティを高めることができる。

【図面の簡単な説明】

【図１】

本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【図２】

図１に示した第１鍵を生成する鍵情報生成方法を説明するための具体例を示した図である。

【図３】

第１鍵の生成する鍵情報生成装置の具体例を示したブロック図である。

【図４】

一般的なＤＥＳ（Data Encryption Standard）暗号化方法に用いられているＳ－Ｂｏｘを示したブロック図である。

【符号の説明】

０１…第１鍵のもとになる情報、０２…第２暗号化装置、

０３…一方向性関数、０４…コンテンツ情報（ディジタル情報）、

０５…第１暗号化装置、０６…暗号化した第１鍵のもとになる情報、

０７…暗号化したディジタル情報、０８…第２復号化装置、

０９…第１鍵のもとになる情報、１０…一方向性関数、

１１…第１復号化装置、１２…コンテンツ情報（ディジタル情報）、

３０…鍵情報生成装置、３１…Ｓ－Ｂｏｘ、３２…論理演算部、

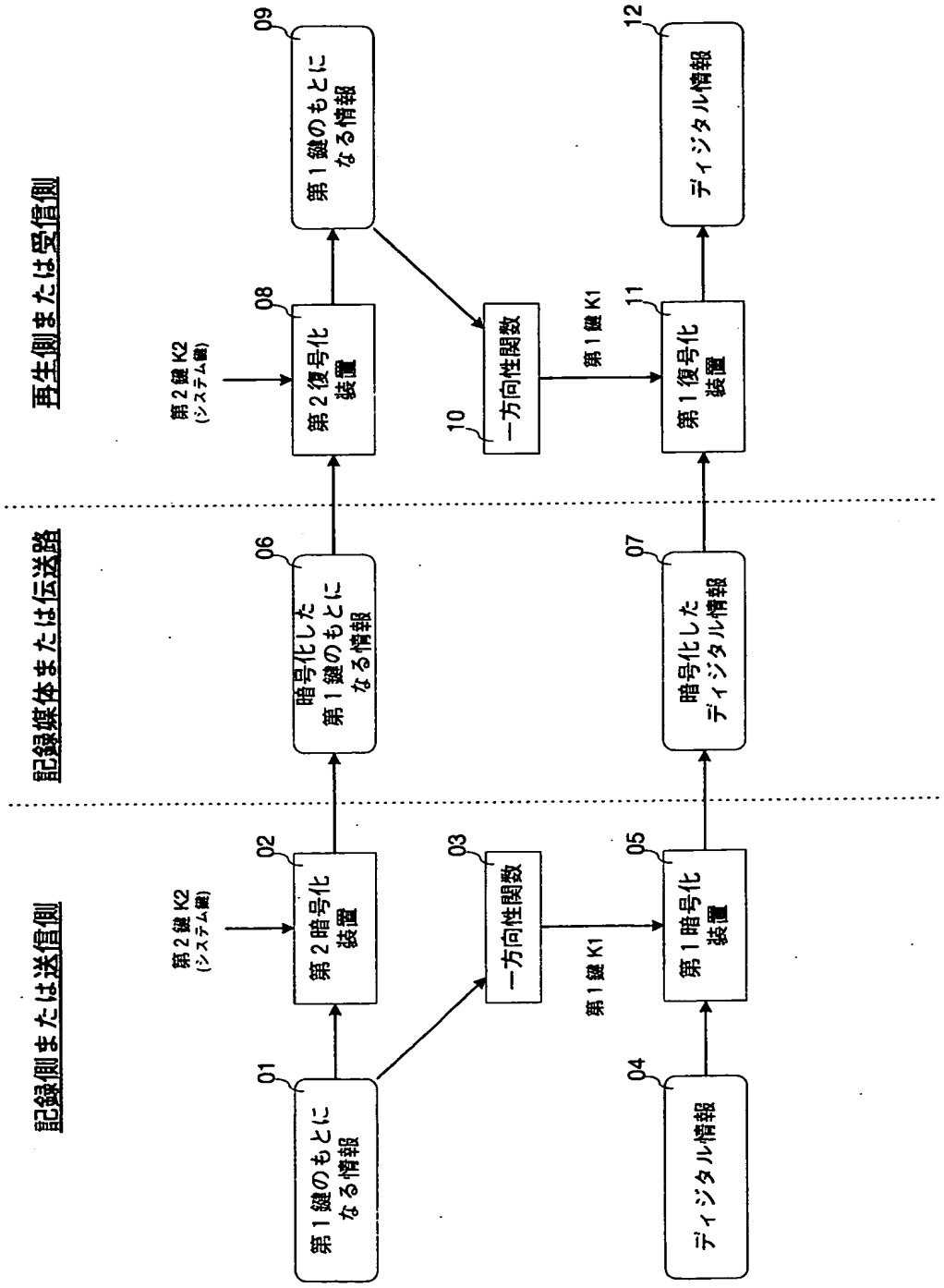
Ｋ１…第１鍵、Ｋ２…第２鍵（システム鍵）、

Ｍ１…第１マトリックス、Ｍ２…第２マトリックス、

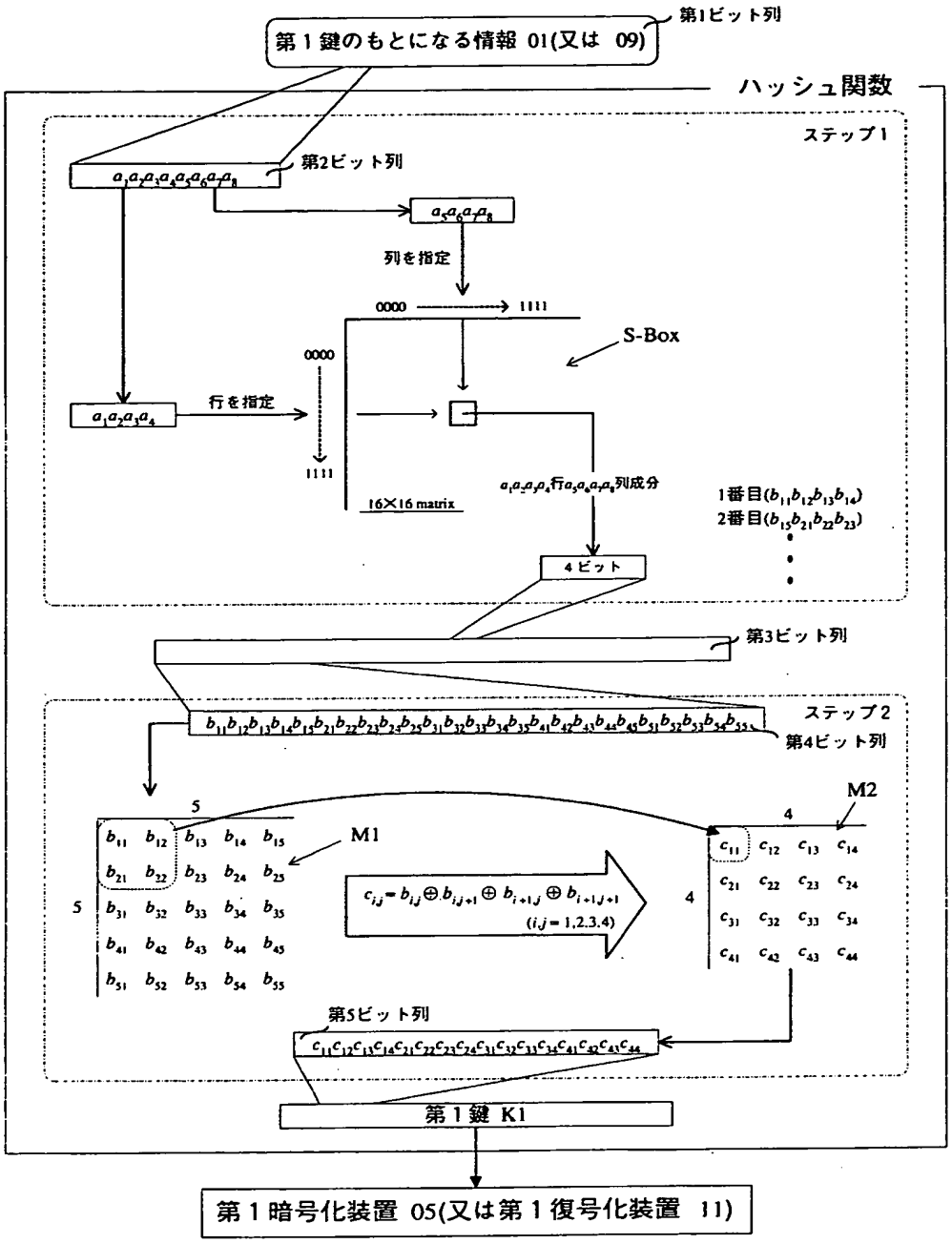
Ｔ…テーブル。

【書類名】　　図面

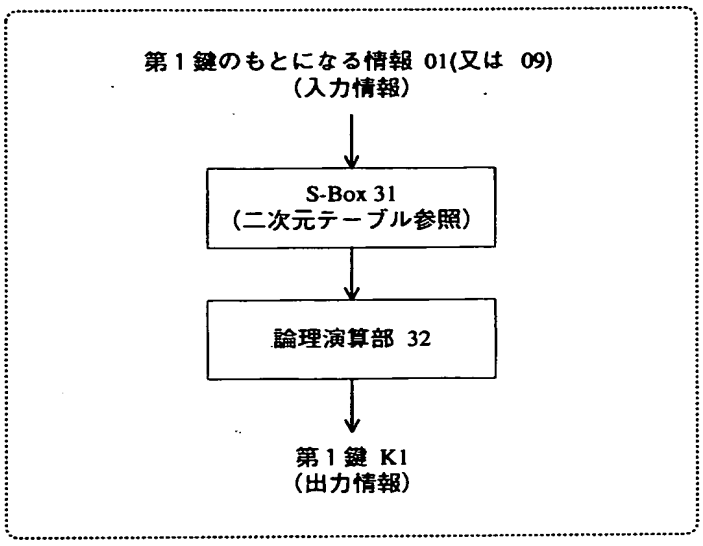
【図１】


記録側または送信側
記録媒体または伝送路
再生側または受信側
01
第１鍵のもとになる情報
02
第２暗号化装置
03
一方向性関数
04
ディジタル情報
05
第１暗号化装置
06
暗号化した第１鍵のもとになる情報
07
暗号化したディジタル情報
08
第２復号化装置
09
第１鍵のもとになる情報
10
一方向性関数
11
第１復号化装置
12
ディジタル情報
第２鍵 K2 (システム鍵)
第１鍵 K1
第２鍵 K2 (システム鍵)
第１鍵 K1

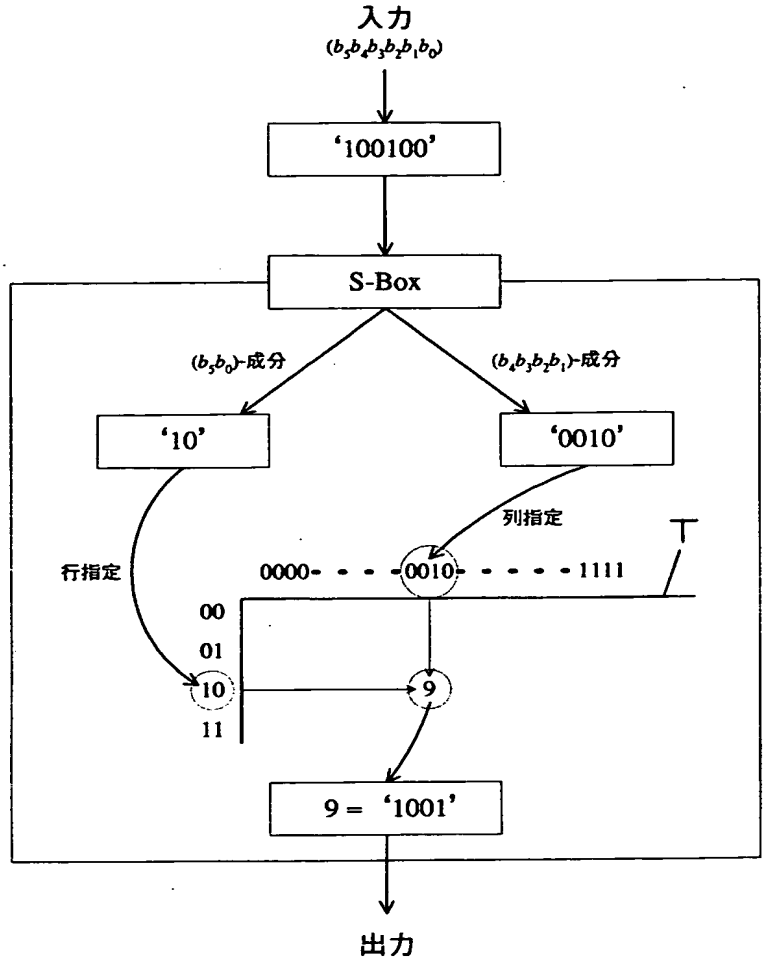
【図２】


第１鍵のもとになる情報 01(又は 09)
第1ビット列
ハッシュ関数
ステップ1
第2ビット列
列を指定
0000
1111
S-Box
行を指定
16×16 matrix
4ビット
1番目($b_{11}b_{12}b_{13}b_{14}$)
2番目($b_{15}b_{21}b_{22}b_{23}$)
第3ビット列
ステップ2
第4ビット列
M2
M1
$c_{ij} = b_{ij} \oplus b_{ij+1} \oplus b_{i+1j} \oplus b_{i+1j+1}$
(i,j = 1,2,3,4)
第5ビット列
第１鍵 K1
第１暗号化装置 05(又は第１復号化装置 11)

【図３】


鍵情報生成装置 30
第１鍵のもとになる情報 01(又は 09)
（入力情報）
S-Box 31
（二次元テーブル参照）
論理演算部 32
第１鍵 K1
（出力情報）

【図４】


入力
$(b_5b_4b_3b_2b_1b_0)$
'100100'
S-Box
(b_5b_0)-成分
$(b_4b_3b_2b_1)$-成分
'10'
'0010'
列指定
行指定
0000- - - -0010- - - - -1111
00
01
10
11
9
9 = '1001'
出力

【書類名】　　要約書

【要約】

【課題】　鍵情報を一方向性関数を用いて生成する。

【解決手段】　第１ビット列よりビット数の少ない第２ビット列に順次分割して入力し、且つ、テーブル内に行と列とに対応させて各要素値を予め設定しておき、各第２ビット列の複数のビットを用いてテーブルの行と列とを指定すると共に、各第２ビット列で指定した行列の部位と対応して得た各要素値を合成した第３ビット列を出力する第１ステップと、第１ステップで出力した第３ビット列を入力するか、又は第３ビット列をこれよりビット数が少ない第４ビット列に分割して入力し、第３又は第４ビット列の各ビットをマトリックス内に配置し、且つ、マトリックス内で第３又は第４ビット列のビット数より少ない複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算した各結果のビットで第３又は第４ビット列のビット数より少ない第５ビット列を出力する第２ステップとからなる。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　　日本ビクター株式会社